

# IAD Top Challenges & Efforts 2016

Neal Ziring, Technical Director Information Assurance Directorate

### SOME MISSION DRIVERS







## Why KEEP TWO LISTS?

#### **Top Challenges List:**

- Advancing the state of the art
- Things we <u>don't know</u> how to do, but need to
- Fundamental new capabilities that we need

Use this list to drive research, innovation, and intellectual capital investment.

#### **Effort Emphasis List:**

- Advancing the state of practice
- Things we know how to do, but <u>aren't getting done</u>
- Get more assurance benefit from existing tools

Use this list to prioritize **staffing**, **publishing**, **policy**, and **partnerships**.

# **Top Challenges 2016**

#	Challenge
C1	Cyber sensing and analysis, adaptable and scalable
C2	Automated risk detection – monitoring, collection, fusion, sense-making
С3	Automated risk mitigation – decision making, orchestration, response actions
C4	Future cryptography – algorithms, protocols, practices
C5	Secure mobility – usable, assured, extending from endpoints to clouds
C6	Distributed cyber situational awareness (multi-domain, multi-event, timely, spanning authorities and sources, etc.)
C7	Predict, measure, and manage the <u>impact</u> of compromises on mission execution (in design & operation)
C8	Optimize and automate detection and mitigation across the kill chain
C9	Internet of Things – how to harden it, use it, defend it, and protect against it
C10	Assured recovery & reconstitution of operational cyber systems
C11	Improve HW and SW assurance for defense systems (incl. weapons platforms)

## **Effort Emphasis List 2016**

#	Effort Emphasis
E1	Deploy IAD innovations to NSA networks
E2	Basic countermeasures for hosts, servers, & services – ensure core mitigations are universally deployed
E3	Eliminate adversary pay-off from phishing
E4	Support defense & mitigations operations directly with analytic results
E5	Authentication - deployment of effective multi-factor authentication (incl. mobile)
E6	Initiate & promote widespread use of standards for cyber information exchange (STIX, TAXII, SWID, etc.)
E7	Improve and modernize key production infrastructure and operations
E8	Secure our own operational environments (IAD and NSA)
E9	CSfC optimization – make CC/NIAP and CSfC work better for customers
E10	Secure network infrastructure against exploitation, at scale
E11	Manage and monitor keys/credentials for CSfC installations